Amendments to the Specification:

Please replace the paragraph starting on page 17 lines 22-27 with the following amended paragraph:

a1

--In operation **506**, a tunnel is generated on the network. Thereafter, information is received at the server from the client utilizing the tunnel, as indicated in operation **508**. Such information is encrypted by the client using the first key. At the server, cryptographic work is performed~~ using the first key~~. See operation **510**. The work may include cryptographic services such as modular exponentiation. In such embodiment, Equation #1 may be employed.--

Please replace the paragraph at page 18 lines 3-10 with the following amended paragraph:

a2

--After the work has been performed, the work results may be encrypted using the first key and sent to the client where it may be decrypted by the client using the first key~~, and the work result can be transmitted to the client~~. A second key comprising at least one parameter for the work performed by the server, such as keys, messages and cyphertext can also be sent to the server. In terms of a business model, payment for the cryptographic service may be based upon a fixed fee. In another aspect of the invention, payment is based upon a per operation payment system. In yet another aspect of the invention, payment is based upon a combination of a fixed fee and a per operation payment system.--

Please replace the paragraph starting on page 18, lines 12-21 with the following amended paragraph:

--Figure **6** is a diagram illustrating the exchange of information **600** between the client and the server in accordance with the method set forth during reference to Figure **5**. As

shown, the first key is initially established between the client and server in operation **602**. Thereafter, in operation **604**, information is received at the server from the client. As set forth earlier, such information is encrypted by the client. A second key ~~is~~ also can be sent to the server from the client in operation **606**. Once the work has been performed, it is sent to the client from the server in operation **608**. In an alternative embodiment, a cryptographic server could be located in a user's server pool, thereby providing for reduced network latency. The management of the cryptographic server would preferably be outsourced.--

Please replace the paragraph starting on page 23, lines 19-28 with the following amended paragraph:

--The querier generates the special modulus *N* and the random base *x* in operation **804**. The particular small prime is used to encode the secret query *j*. The database computes a modular exponentiation using *n* and *x*, where the exponent is the product of a number of small primes. Exactly which small prime is selected is a function of the bits in the database that are one[']s and zero[']s. The final result is a single value which is ~~bigger~~ no larger than *N*. The querier takes this final result and performs a test on it to determine the result of the query. The test is a modular exponentiation that uses the result of the query as the base. In operation **806**, the querier's query is "hidden" among the set of m possible queries (i.e., placed in a batch with the other queries).--

Please replace the paragraph starting on page 23, line 30 through page 24, line 8 with the following amended paragraph:

--Notice that the communication between the querier and the database is the size of a single ~~1024-bit~~ number no larger than *N* no matter how large the database is. Notice that this compression in communication is achieved at the expense of an increase in computation by both parties. Specifically, both parties must perform modular exponentiations of a specific type. These are not modular exponentiations to encrypt,

decrypt, sign or verify a signature. Instead, there are modular exponentiations in the service of a complex protocol to perform a sophisticated cryptographic service (private information retrieval). The queries are sent to the database or other data source in operation **808,** and responses to the queries are received in operation **810**.--

a3

Please replace the paragraph starting on page 24, lines 10-24 with the following amended paragraph:

--It is possible to reduce the computation for the database by restricting the database to 100,000 elements and performing the private information retrieval over that set of bits. This hides the true query in a smaller set of possible queries. The communication size remains the same, but the computation that the database must perform is reduced. The computation that the database must perform is dominated by the cost of performing a modular exponentiation where the exponent is a product of as many small primes as there are one[']s in that portion of the database. The smaller the portion of the database within which the query is hidden, the fewer small primes in the exponent product, and thus the simpler the calculation for the database, which is referred to as "per-tree" pricing. This is very different from having the database simply retrieve 100,000 answers for the querier. It is a complex protocol for private information retrieval which restricts the possible queries over which the protocol takes place in order to reduce the computational burden on the service provider. The response to the query is separated from the responses in operation **812**.--

Please replace the paragraph starting on page 25, lines 3-9 with the following amended paragraph:

a4

--According to an embodiment of the present invention, a participant proves to be one of a plausible set of m possible participants without revealing which, where *m* is a tunable parameter. There is also a non-interactive version of this called a "group signature". An illustrative cryptographic solution requires the participant and the verifier to each perform

a4

about *m* modular exponentiations, and exchange one round of communication of size <u>proportional to</u> *m*. This example has many practical applications, including to enhance the value of recommendation systems.--